A new large class of functions not APN infinitely often

Florian Caullery

A NEW LARGE CLASS OF FUNCTIONS NOT APN INFINITELY OFTEN

FLORIAN CAULLERY

Abstract. In this paper, we show that there is no vectorial Boolean function of degree $4e$, with e satisfaying certain conditions, which is APN over infinitely many extensions of its field of definition. It is a new step in the proof of the conjecture of Aubry, McGuire and Rodier. Vectorial Boolean function and Almost Perfect Non-linear functions and Algebraic surface and CCZ equivalence

1. Introduction

A vectorial Boolean function is a function $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$. This object arises in fields like cryptography and coding theory and is of particular interest in the study of block-ciphers using a substitution-permutation network (SP-network) since they can represent a Substition Box (S-Box). In 1990 Biham and Shamir introduced the differential cryptanlysis in [3]. The basic idea is to analysis how a difference between two inputs of an S-box will influence the difference between the two outputs. This attack was the motivation for Nyberg to introduce the notion of Almost Perfectly Nonlinear (APN) function [22] which are the function providing the S-Boxes with best resistance to the differential cryptanalysis. An APN function is a vectorial Boolean function such that $\forall a \neq 0, b \in \mathbb{F}_{2^m}$ there exist at most two solutions to the equation:

$$f(x + a) + f(x) = b$$

The problem of the classification of all APN functions is challenging and has been studied by many authors. In a first time, the studies focused on power functions and it was recently extended to polynomial functions (Carlet, Pott and al [7, 12, 13]) or polynomials on small fields (Dillon [9]). On the other hand, several authors (Berger, Canteaut, Charpin, Laigle-Chapuy [2], Byrne, McGuire [6] or Jedlicka [18]) showed that APN functions cannot exist in certain cases. Some also studied the APN functions on fields of odd characteristic (Leducq [20], Pott and al. [11, 23], Ness, Helleseth [21] or Wang, Zha [26, 27]).

One way to approach the problem of the classification is to consider the function APN over infinitely many extensions of $\mathbb{F}_2$, namely, the exceptional APN functions. The two best known exceptional APN functions are the Gold functions: $f(x) = x^{2^i+1}$ and the Kasami functions $f(x) = x^{4^i-2^i+1}$, both are APN whenever i and m are coprime. We will refer to $2^i + 1$ and $4^i - 2^i + 1$ respectively as the Gold and Kasami exponent. It was proved by Hernando and McGuire in [15] that those two

Date: September 30, 2013.

Institut de Mathématiques de Luminy, CNRS-UPR9016, 163 av. de Luminy, case 907, 13288 Marseille Cedex 9, France.

Email: florian.caullery@etu.univ-amu.fr.

functions are the only monomial exceptional APN functions. It was the starting point for Aubry, McGuire and Rodier to formulate the following conjecture:

Conjecture 1. *([1]) The only exceptional APN functions are, up to Carlet Charpin Zinoviev-equivalence (as defined below), the Gold and Kasami functions.*

We provide the definition of the Carlet Charpin Zinoviev equivalence:

Definition 1. *([7]) Two functions f and g are Carlet Charpin Zinoviev (CCZ-)equivalent if there exist a linear permutation between their graphs (i.e. the sets $\{x, f(x)\}$ and $\{x, g(x)\}$).*

It has to be noted that all the functions CCZ-equivalent to an APN function are also APN [7].

By means of a simple rewriting of the definition of APN function in terms of algebraic geometry, Rodier was able to prove that, if the projective closure of the surface X defined by the equation:

$$\frac{f(x) + f(y) + f(z) + f(x + y + z)}{(x + y)(y + z)(z + x)} = 0$$

has an absolutely irreducible component defined over $\mathbb{F}_{2^m}$, then f is not an exceptional APN function [24]. The idea now is to exploit this criteria to prove that the functions which are not CCZ-equivalent to a Gold or Kasami function are not exceptional APN. This approach enabled Aubry, McGuire and Rodier to state, for example, that there is no exceptional APN function of degree odd not a Gold or Kasami exponent and of degree $2e$ with e an odd number [1].

From now on we let $q = 2^m$,

$$\phi(x, y, z) = \frac{f(x) + f(y) + f(z) + f(x + y + z)}{(x + y)(y + z)(z + x)}$$

and

$$\phi_i(x, y, z) = \frac{x^i + y^i + z^i + (x + y + z)^i}{(x + y)(y + z)(z + x)}$$

In this paper we continue in the same way than Aubry, McGuire and Rodier and are interested in the functions of degree $4e$ with e such that ϕ_e is absolutely irreducible. As shown by Janwa and al. ([17] and [16]) it is the case for example when $e \equiv 3 \pmod 4$ or when $e \equiv 5 \pmod 8$ and the maximum cyclic code of length $\frac{e-1}{4}$ has no codewords of weight 4. In particular, e cannot be a Gold or a Kasami exponent. There are many others e which satisfy the condition. It was even conjectured that it was the case of any e odd not a Gold or Kasami exponent but $e = 205$ was shown to be the smallest counter-example by Hernando and McGuire [15]. We now give an overview of the classification of the exceptional APN function.

2. The state of the art

Using the approach described in the introduction Aubry, McGuire and Rodier obtained the following results in [1].

Theorem 1. ***(Aubry, McGuire and Rodier,** [1]) If the degree of the polynomial function f is odd and not an exceptional number then f is not an exceptional APN function.*

Theorem 2. ***(Aubry, McGuire and Rodier*** [1]***)*** *If the degree of the polynomial function f is $2e$ with e odd and if f contains a term of odd degree, then f is not an exceptional APN function.*

There are some results in the case of Gold degree $2^i + 1$:

Theorem 3. ***(Aubry, McGuire and Rodier*** [1]***)*** *Suppose $f(x) = x^{2^i+1} + g(x)$ where $\deg(g) \leqslant 2^{i-1} + 1$. Let $g(x) = \sum_{j=0}^{2^{i-1}+1} a_j x^j$. Suppose moreover that there exists a nonzero coefficient a_j of g such that $\phi_j(x, y, z)$ is absolutely irreducible. Then f is not an exceptional APN function.*

This result has been consequently extended by Delgado and Janwa in [10] with the two following theorems:

Theorem 4. ***(Delgado and Janwa*** [10]***)*** *For $k \geq 2$, let $f(x) = x^{2^i+1} + h(x) \in \mathbb{F}_q$ where $deg(h) \equiv 3 \pmod 4 < 2^i + 1$. Then f is not an exceptional APN function.*

and

Theorem 5. ***(Delgado and Janwa*** [10]***)*** *For $k \geq 2$, let $f(x) = x^{2^i+1} + h(x) \in \mathbb{F}_q$ where $deg(h) = d \equiv 1 \pmod 4 < 2^i + 1$. If ϕ_{2^i+1}, ϕ_d are relatively prime, then f is not an exceptional APN function.*

There also exist a result for polynomials of Kasami degree $2^{2i} - 2^i + 1$:

Theorem 6. ***(Férard, Oyono and Rodier*** [14]***)*** *Suppose $f(x) = x^{2^{2i}-2^i+1} + g(x)$ where $\deg(g) \leqslant 2^{2k-1} - 2^{k-1} + 1$. Let $g(x) = \sum_{j=0}^{2^{2k-1}-2^{k-1}+1} a_j x^j$. Suppose moreover that there exist a nonzero coefficient a_j of g such that $\phi_j(x, y, z)$ is absolutely irreducible. Then f is not an exceptional APN function.*

Rodier proved the following results in [25]. We recall that for any function $f : \mathbb{F}_q \to \mathbb{F}_q$ we associate to f the polynomial $\phi(x, y, z)$ defined by:

$$\phi(x, y, z) = \frac{f(x) + f(y) + f(z) + f(x + y + z)}{(x + y)(x + z)(y + z)}.$$

Theorem 7. ***(Rodier*** [25]***)*** *If the degree of a polynomial function f is such that $\deg(f) = 4e$ with $e \equiv 3 \pmod 4$, and if the polynomials of the form*

$$(x + y)(x + z)(y + z) + R,$$

with

$$R(x, y, z) = c_1\left(x^2 + y^2 + z^2\right) + c_4(xy + xz + zy) + b_1(x + y + z) + d_1,$$

for $c_1, c_4, b_1, d \in \mathbb{F}_{q^3}$, do not divide ϕ, then f is not an exceptional APN function.

There are more precise results for polynomials of degree 12.

Theorem 8. ***(Rodier*** [25]***)*** *If the degree of the polynomial f defined over $\mathbb{F}_q$ is 12, then either f is not an exceptional APN function or f is CCZ-equivalent to the Gold function x^3.*

3. Our main Result

The goal of this paper is to prove the following result:

Theorem 9. *Let $f : \mathbb{F}_q \to \mathbb{F}_q$ of degree $4e$ with $e > 3$ such that ϕ_e is absolutely irreducible. Then f is not an exceptional APN function.*

The proof of this theorem is decomposed in two main steps. The first one is to show that the exceptional APN functions of degree as in the conditions of theorem 9 must be of a certain form. The second one is to prove that they are hence CCZ-equivalent to a nonexceptional APN function, which is a contradiction.

4. The divisibility condition

In the statement of theorem 7 in [25] the condition that e must be $3 \pmod 4$ is only used to guarantee that ϕ_e is absolutely irreducible (as shown in [17]). It is easy to see that the proof works whenever e is such that ϕ_e is absolutely irreducible. As a consequence of this remark theorem 7 can be directly extended as follow:

Theorem 10. *Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be of degree $d = 4e$ with e such that ϕ_e is absolutely irreducible. If the polynomials of the form*

$$(x+y)(x+z)(y+z) + R(x,y,z),$$

with

$$R(x,y,z) = c_1\left(x^2+y^2+z^2\right) + c_4(xy+xz+zy) + b_1(x+y+z) + d,$$

for $c_1, c_4, b_1, d_1 \in \mathbb{F}_{q^3}$, does not divide ϕ then f is not an exceptional APN function.

Remark. *As said in the introduction, ϕ_e is absolutely irreducible in many cases including $e \equiv 3 \pmod 4$.*

Remark. *Among the examples where ϕ_e is not absolutely irreducible, we would like to draw attention on two particular cases. Firstly, one can quickly verify that ϕ_e is not irreducible when e is even (see [1] lemma 2.2). Secondly, when e is a Gold or a Kasami exponent there exists a decomposition of ϕ_e into absolutely irreducible factors (see [17]).*

We will now investigate the consequences of the last theorem.

Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function of degree $d = 4e$ where $e > 3$ is odd and such that ϕ_e is absolutely irreducible. Suppose now that f is an exceptional APN function. We recall that

$$\phi(x,y,z) = \frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(y+z)(z+x)},$$

Writing $f(x) = \sum_{i=0}^{d} a_i x^i$ we have

$$\phi_f = \sum_{i=0}^{d} a_i \phi_i,$$

We can fix a_d to 1 without loss of generality as $\mathbb{F}_q$ is a field.

Let ρ be a generator of the Galois group $\mathrm{Gal}\left(\mathbb{F}_{q^3}/\mathbb{F}_q.\right)$ and let us consider $c_1, c_4, b_1, d_1 \in \mathbb{F}_{q^3}$, $R(x,y,z) = c_1\left(x^2+y^2+z^2\right) + c_4(xy+xz+zy) + b_1(x+y+z) + d$ and $A = (x+y)(y+z)(z+x)$.

As a consequence of theorem 10, we may assume that the polynomial $P = (A+R)(A+\rho(R))\left(A+\rho^2(R)\right)$ divides ϕ. We denote P_i the homogeneous component of degree i of P. As ϕ is of total degree $d-3$, there exists a polynomial $Q \in \mathbb{F}_{q^3}[x,y,z]$ of total degree $d-12$ such that $\phi = P \times Q$. Denoting Q_i the homogeneous component of Q of degree i we get

$$\sum_{i=0}^{9} P_i \cdot \sum_{i=0}^{d-12} Q_i = \sum_{i=0}^{d} a_i \phi_i.$$

As ϕ is a symmetrical polynomial in x, y, z we can write it using symmetrical functions $s_1 = x+y+z$, $s_2 = xy+xz+yz$ and $s_3 = xyz$ (see [4] chapter 6). Denoting $p_i = x^i + y^i + z^i$, we have $p_i = s_1 p_{i-1} + s_2 p_{i-2} + s_3 p_{i-3}$. We remark that $\phi_i = \frac{p_i + s_1^i}{A}$ and that $A = (x+y)(y+z)(z+y) = s_1 s_2 + s_3$.

We shall now determine all the coefficients of R identifying degree by degree P, Q and ϕ.

Proposition 1. *If $A+R$ divides ϕ_f, then $R = c_1\phi_5 + c_1^3$ and the trace of c_1 in $\mathbb{F}_{q^3}$ is 0. Moreover the polynomial $(A+R)(A+\rho(R))\left(A+\rho^2(R)\right)$ is equal to*

$$\frac{L(x)^3 + L(y)^3 + L(z)^3 + L(x+y+z)^3}{(x+y)(y+z)(z+x)}$$

where $L(x) = x(x+c_1)(x+\rho(c_1))\left(x+\rho^2(c_1)\right)$.

Proof. We will need the following lemmas :

Lemma 1. *Suppose $e \equiv 3 \pmod 4$ and let $s = x+y$. We have :*

$$(x+z)^2\phi_e = \left(x^{e-1}+z^{e-1}\right) + s\frac{\left(x^{e-2}z + z^{e-2}x\right)}{x+z} + s^2\frac{\left(x^{e-3}+z^{e-3}\right)\left(x^2+z^2+xz\right)}{(x+z)^2} \pmod{s^3}$$

Proof. We have

$$A\phi_e = x^e + y^e + z^e + (x+y+z)^e.$$

Let us put $s = y+z$. We get

$$\begin{aligned} & (x+z)(s+x+z)s\phi_e \\ = \; & x^e + (s+z)^e + z^e + (x+s)^e \\ = \; & s\left(x^{e-1}+z^{e-1}\right) + s^2\left(x^{e-2}+z^{e-2}\right) + s^3\left(x^{e-3}+z^{e-3}\right) \pmod{s^4}. \end{aligned}$$

Hence

(1)
$$s(x+z)\phi_e + (x+z)^2\phi_e = \left(x^{e-1}+z^{e-1}\right) + s\left(x^{e-2}+z^{e-2}\right) + s^2\left(x^{e-2}+z^{e-2}\right) + s^3\left(x^{e-3}+z^{e-3}\right) \pmod{s^4}.$$

As we have

$$(x+z)^2\phi_e = \left(x^{e-1}+z^{e-1}\right) \pmod{s},$$

and hence

$$(x+z)\phi_e = \frac{x^{e-1}+z^{e-1}}{x+z} \pmod{s},$$

we deduce

$$\begin{aligned}
(x+z)^2\phi_e &= \left(x^{e-1}+z^{e-1}\right)+s\left(x^{e-2}+z^{e-2}\right)+s\left(x+z\right)\phi_e \pmod{s^2}\\
&= \left(x^{e-1}+z^{e-1}\right)+s\left(x^{e-2}+z^{e-2}\right)+s\frac{x^{e-1}+z^{e-1}}{x+z} \pmod{s^2}\\
&= \left(x^{e-1}+z^{e-1}\right)+s\frac{x^{e-2}z+z^{e-2}x}{x+z} \pmod{s^2}.
\end{aligned}$$

So we have

$$(x+z)^2\phi_e = \left(x^{e-1}+z^{e-1}\right)+s\frac{x^{e-2}z+z^{e-2}x}{x+z} \pmod{s^2} \tag{2}$$

and

$$(x+z)\phi_e = \frac{\left(x^{e-1}+z^{e-1}\right)}{x+z}+s\frac{x^{e-2}z+z^{e-2}x}{(x+z)^2} \pmod{s^2}. \tag{3}$$

Using 2 and 3 in 1 we get

$$\begin{aligned}
(x+z)^2\phi_e &= \left(x^{e-1}+z^{e-1}\right)+s\left(x+z\right)\phi_e+s\left(x^{e-2}+z^{e-2}\right)+s^2\left(x^{e-3}+z^{e-3}\right) \pmod{s^3}\\
&= \left(x^{e-1}+z^{e-1}\right)+s\frac{\left(x^{e-1}+z^{e-1}\right)}{x+z}+s^2\frac{x^{e-2}z+z^{e-2}x}{(x+z)^2}+s\left(x^{e-2}+z^{e-2}\right)+\\
&\quad s^2\left(x^{e-3}+z^{e-3}\right) \pmod{s^3}\\
&= \left(x^{e-1}+z^{e-1}\right)+s\frac{\left(x^{e-2}z+z^{e-2}x\right)}{x+z}+s^2\frac{\left(x^{e-3}+z^{e-3}\right)\left(x^2+z^2+xz\right)}{(x+z)^2} \pmod{s^3}.
\end{aligned}$$

□

Lemma 2. *Suppose* $e \equiv 1 \pmod 4$ *and let* $s = x+y$. *We have :*

$$(x+z)^2\phi_e = \left(x^{e-1}+z^{e-1}\right)+s\frac{\left(x^{e-1}+z^{e-1}\right)}{x+z}+s^2\frac{\left(x^{e-1}+z^{e-1}\right)}{(x+z)^2} \pmod{s^3}$$

Proof. The proof of lemma 2 is similar to the proof of lemma 1. □

Lemma 3. *For all odd* $e \in \mathbb{N}$ *we have*

$$\phi_e(x,z,z) = \frac{x^{e-1}+z^{e-1}}{(x+z)^2}$$

The proof is straightforward from previous lemma. It can also be found in [10]
For all $k \in \{0,1,\ldots,d\}$ we have

$$a_k\phi_k = \sum_{i=0}^{9} P_iQ_{k-i-3}.$$

Degree $d-3$

We have

$$\phi_d = A^3\phi_e^4 = P_9Q_{d-12}.$$

As $P_9 = A^3$, we get $Q_{d-12} = \phi_e^4$.

Degree $d-4$

We have
$$a_{d-1}\phi_{d-1} = P_9 Q_{d-13} + P_8 Q_{d-12}.$$
As $P_8 = A^2(s_1^2\mathrm{tr}(c_1) + s_2\mathrm{tr}(c_4))$, it gives us
$$a_{d-1}\phi_{d-1} = A^3 Q_{d-13} + A^2\phi_e^4(s_1^2\mathrm{tr}(c_1) + s_2\mathrm{tr}(c_4)).$$
By lemma 3 ϕ_{d-1} is not divisible by A, so $a_{d-1} = 0$ and
$$AQ_{d-13} = \phi_e^4(s_1^2\mathrm{tr}(c_1) + s_2\mathrm{tr}(c_4)).$$
We know that A is prime with $s_1^2\mathrm{tr}(c_1) + s_2\mathrm{tr}(c_4)$ because $(x + y)$ does not divide this polynomial, and A does not divide either ϕ_5^4, which implies $Q_{d-13} = P_8 = 0$ and $\mathrm{tr}(c_1) = \mathrm{tr}(c_4) = a_{d-1} = 0$.

Degree $d - 5$

We have
$$a_{d-2}\phi_{d-2} = a_{d-2}(A\phi_{2e-1}^2) = P_9 Q_{d-14} + P_8 Q_{d-13} + P_7 Q_{d-12}.$$
Knowing that $P_8 = Q_7 = 0$ we obtain
$$a_{d-2}(A\phi_{2e-1}^2) = P_9 Q_{d-14} + P_7 Q_{d-12}.$$
We also know that
$$P_7 = A(s_1^4 q_1(c_1) + s_2^2 q_1(c_4) + s_1^2 s_2 q_5(c_1, c_4)) + A^2 s_1 \mathrm{tr}(b_1),$$
denoting

$q_1(c_i) = c_i\rho(c_i) + c_i\rho^2(c_i) + \rho(c_i)\rho^2(c_i)$ and

$q_5(c_1, c_4) = c_1(\rho(c_4) + \rho^2(c_4)) + c_4(\rho(c_1) + \rho^2(c_1)) + \rho(c_1)\rho^2(c_4) + \rho(c_4)\rho^2(c_1)$.

So
$$a_{d-2}\phi_{2e-1}^2 = A^2 Q_{d-14} + \phi_e^4(s_1^4 q_1(c_1) + s_2^2 q_1(c_4) + s_1^2 s_2 q_5(c_1, c_4) + As_1\mathrm{tr}(b_1)), \tag{4}$$
Putting $y = z$ we have
$$a_{d-2}\left(\frac{x^{4e-4} + z^{4e-4}}{(x+z)^4}\right) + \left(\frac{x^{4e-4} + z^{4e-4}}{(x+z)^8}\right)(q_1(c_1)x^4 + q_1(c_4)z^4 + x^2z^2 q_5(c_1, c_4)) = 0,$$
hence we obviously have $q_5(c_1, c_4) = 0$ and $q_1(c_1) = q_1(c_4) = a_{d-2}$. We do not assume that $y = z$ anymore.

We know from (4) that A divides $a_{d-2}(\phi_{2e-1}^2 + \phi_e^4(s_1^4 + s_2^2))$, as it is a square, A^2 divides it too. Replacing in (4) we get
$$a_{d-2}(\phi_{2e-1}^2 + \phi_e^4(s_1^4 + s_2^2))^2 + A^2 Q_{d-14} = A\phi_e^4 s_1 \mathrm{tr}(b_1),$$
so A divides $\mathrm{tr}(b_1)s_1\phi_e^4$. But A divides neither s_1 nor ϕ_e^4 so $\mathrm{tr}(b_1) = 0$. In conclusion we have
$$P_7 = q_1(c_1)(s_1^2 + s_2)^2 A = q_1(c_1)A\phi_5^2. \quad \text{and}$$
$$Q_{d-14} = q_1(c_1)\frac{\phi_{2e-1}^2 + \phi_e^4\phi_5^2}{A^2}.$$

Lemma 4. *The polynomial $Q_{d-14}(x, z, z)$ is equal to zero.*

Proof. from lemma 2 and 1 we get, if either $e \equiv 3 \pmod 4$ or $e \equiv 1 \pmod 4$:

$$Q_{d-14} = \left(\frac{\left(\frac{x^{2e-2}+z^{2e-2}}{(x+z)^2} + s\left(\frac{x^{2e-2}+z^{2e-2}}{(x+z)^3}\right) + s^2R_1\right)}{A}\right)^2 +$$

$$\left(\frac{\left(\frac{x^{2e-2}+z^{2e-2}}{(x+z)^4} + s^2R_2\right)((x+z)^2 + s(x+z) + s^2)}{A}\right)^2$$

$$= \frac{s}{(x+y)(x+z)}R_3,$$

hence $Q_{d-14}(x,z,z) = 0$. □

Degree $d-6$

We have

$$a_{d-3}\phi_{d-3} = P_9Q_{d-15} + P_8Q_{d-14} + P_7Q_{d-13} + P_6Q_{d-12} = P_9Q_{d-15} + P_6Q_{d-12}.$$

We know that

$$P_6 = A^2\mathrm{tr}(d_1) + A(s_1^3q_5(c_1,b_1) + s_1s_2q_5(c_1,b_1)) + s_1^6N(c_1) + s_1^4s_2q_4(c_1,c_4) + s_1^2s_2^2q_4(c_4,c_1) + s_2^3N(c_4)$$

where

$$N(a) = a\rho(a)\rho^2(a)\text{which is the norm of a in } \mathbb{F}_q,$$
$$q_4(a,b) = a\rho(a)\rho^2(b) + a\rho(b)\rho^2(a) + b\rho(a)\rho^2(a)$$

and

$$q_5(a,b) = a(\rho(b) + \rho^2(b)) + b(\rho(a) + \rho^2(a)) + \rho(a)\rho^2(b) + \rho(b)\rho^2(a),$$

for all a, b in $\mathbb{F}_{q^3}$.

Making $y = z$ we get:

$$a_{d-3}\phi_{d-3}(x,z,z) = P_6(x,z,z)\phi_e^4(x,z,z),$$

with

$$P_6(x,z,z) = (c_1x^2 + c_4z^2)(\rho(c_1)x^2 + \rho(c_4)z^2)(\rho^2(c_1)x^2 + \rho^2(c_4)z^2).$$

As

$$\phi_{d-3}(x,z,z) = \frac{x^{d-4}+z^{d-4}}{(x+z)^2}$$

and

$$\phi_e^4(x,z,z) = \frac{x^{d-4}+z^{d-4}}{(x+z)^8},$$

we have

$$(c_1x^2 + c_4z^2)(\rho(c_1)x^2 + \rho(c_4)z^2)(\rho^2(c_1)x^2 + \rho^2(c_4)z^2) = a_{d-3}(x+z)^6.$$

Hence $c_1 = c_4$.
Now we have

$$N(c_1)\left(\phi_{d_3} + \phi_5^3\phi_e^4\right) = A^3Q_{d-15} + \mathrm{tr}(d_1)A^2\phi_e^4 + q_5(c_1,b_1)A\phi_5s_1\phi_e^4. \tag{5}$$

One can verify with lemma 1 and 2 that A^2 divides $\phi_{d_3}+\phi_5^3\phi_e^4$ and we obtain $q_5(c_1,b_1)=0$ since $\phi_5 s_1\phi_e^4$ is prime with A. Plugging the last result into 5 and dividing the whole expression by A^2 we get

$$AQ_{d-15}=N(c_1)\frac{\left(\phi_{d_3}+\phi_5^3\phi_e^4\right)}{A^2}+\mathrm{tr}(d_1)\phi_e^4.$$

Putting $y=z$, we obtain

$$N(c_1)\frac{\left(\phi_{d_3}+\phi_5^3\phi_e^4\right)}{A^2}(x,z,z)=\mathrm{tr}(d_1)\phi_e^4(x,z,z).$$

Now either $\frac{\left(\phi_{d_3}+\phi_5^3\phi_e^4\right)}{A^2}(x,z,z)$ is different from $\phi_e^4(x,z,z)$ and $\mathrm{tr}(d_1)=N(c_1)=0$, or $\frac{\left(\phi_{d-3}+\phi_5^3\phi_e^4\right)}{A^2}(x,z,z)=\phi_e(x,z,z)$ and $\mathrm{tr}(d_1)=N(c_1)$ but in both case we have $\mathrm{tr}(d_1)=N(c_1)$.

Degree $d-7$

We have

$$a_{d-4}\phi_{d-4}=P_9Q_{d-16}+P_8Q_{d-15}+P_7Q_{d-14}+P_6Q_{d-13}+P_5Q_{d-12}, \tag{6}$$

where

$$P_5=q_4(c_1,b_1)s_1\phi_5^2+A(q_1(b_1)s_1^2+q_5(c_1,d_1)\phi_5),$$

We know that $\phi_{d-4}=A^7\phi_{\frac{e-1}{2}}$ so making again $y=z$ enables us to obtain:

$$0=P_5(x,z,z)=q_4(c_1,b_1)(x(x^2+z^2))$$

and finally $q_4(c_1,b_1)=0$. Now 6 becomes

$$a_{d-4}A^7\phi_{\frac{e-1}{2}}=A^3Q_{d-16}+q_1(c_1)A\phi_5^2Q_{d-14}+\left(q_1(b_1)s_1^2+q_5(c_1,d_1)\phi_5\right)A\phi_e^4.$$

We divide this expression by A and we put $y=z$ and it gives

$$q_1(b_1)x^2=q_5(c_1,d_1)(x^2+y^2),$$

so $q_1(b_1)=q_5(c_1,d_1)=0$.

degree $d-8$

For this step we have:

$$a_{d-5}\phi_{d-5}=P_9Q_{d-17}+P_8Q_{d-16}+P_7Q_{d-15}+P_6Q_{d-14}+P_5Q_{d-13}+P_4Q_{d-12}.$$

with

$$P_4=q_4(b_1,c_1)s_1^2\phi_5+q_4(c_1,d_1)\phi_5^2+q_5(b_1,d_1)As_1,$$

Putting $y=z$ we get:

$$\begin{aligned}a_{d-5}\frac{x^{d-6}+z^{d-6}}{(x+z)^2}&=\frac{1}{(x+z)^8}((q_4(b_1,c_1)+q_4(c_1,d_1))(x^d+x^4z^{d-4})+\\&\qquad q_4(b_1,c_1)(x^{d-2}z^2+x^2z^{d-2})+q_4(c_1,d_1)(x^{d-4}z^4+z^d)).\end{aligned}$$

Putting on the same denominator we have

$$a_{d-5}(x^{d-6}z^6+x^6z^{d-6})=0$$

and then $a_{d-5}=0$, therefore $q_4(b_1,c_1)=q_4(c_1,d_1)=0$

Summary
At this point we get the following system

$$\begin{cases} q_1(b_1) = 0 \\ \mathrm{tr}(b_1) = 0 \\ q_5(c_1, b_1) = 0 \\ \mathrm{tr}(c_1) = 0 \\ q_4(c_1, b_1) = 0 \\ q_4(b_1, c_1) = 0 \\ q_4(c_1, d_1) = 0 \\ q_5(c_1, d_1) = 0 \\ \mathrm{tr}(d_1) = N(c_1) \end{cases}$$

Let us suppose that $c_1 \neq 0$. The linear system in $b_1, \rho(b_1), \rho^2(b_1)$ formed by the three first equations gives $b_1 = 0$. Indeed, the determinant of this system is $(c_1 + \rho(c_1))(\rho(c_1) + \rho^2(c_1))(\rho^2(c_1) + c_1)$ can vanish only if $c_1 = 0$ because $\mathrm{tr}(c_1) = 0$.

If, moreover, $c_1 \neq \rho(c_1)$, the last 3 equations form a linear system in $d_1, \rho(d_1), \rho^2(d_1)$ which can gives

$$d_1 = c_1^3.$$

Therefore $R = c_1\phi_5^2 + c_1^3$ which is the form given in the proposition 4.

If $c_1 = \rho(c_1)$ then, as $\mathrm{tr}(c_1) = 0$, $c_1 = 0$. Let us suppose from now on that it is the case. We need to use

$$a_{d-6}\phi_{d-6} = P_9Q_{d-18}+P_8Q_{d-17}+P_7Q_{d-16}+P_6Q_{d-15}+P_5Q_{d-14}+P_4Q_{d-13}+P_3Q_{d-12},$$

when we replace c_1 by zero we get

$$a_{d-6}A\phi_{2e-1}^2 = A^3Q_{d-18} + P_3\phi_e^4,$$

where

$$P_3 = N(b_1)s_1^3 + q_1(d_1)A.$$

If moreover we make $y = z$ we obtain

$$0 = P_3(x, z, z) = N(b_1)x^3.$$

so $N(b_1) = 0$. Therefore $b_1 = 0$.

We now use

$$\begin{aligned} a_{d-9}\phi_{d-9} = P_9Q_{d-21}+P_8Q_{d-20}+P_7Q_{d-19}+P_6Q_{d-18}+P_5Q_{d-17}+P_4Q_{d-16}+P_3Q_{d-15}+ \\ P_2Q_{d-14} + P_1Q_{d-13} + P_0Q_{d-12}, \end{aligned}$$

which gives:

$$a_{d-9}\phi_{d-9} = A^3Q_{d-21} + N(d_1)\phi_e^4.$$

If we put $y = z$ we obtain

$$a_{d-9}\frac{x^{d-10} + z^{d-10}}{(x+z)^2} = N(d_1)\frac{x^{d-4} + z^{d-4}}{(x+z)^8}.$$

Putting on the same denominator we get $a_{d-9} = 0$ and therefore $N(d_1) = 0$, hence $d_1 = 0$. It means that $R = 0$, finally proving the first part of proposition 1.

Now let us consider $L(x) = x(x+c_1)(x+\rho(c_1))\left(x+\rho^2(c_1)\right)$, since $\operatorname{tr}(c_1) = 0$, L is a q-affine polynomial and as $L(x)$ has only one root of 0 in $\mathbb{F}_q$ (that is $x = 0$), $L(x)$ is a q-affine permutation. One can verify that

$$\frac{L(x)^3 + L(y)^3 + L(z)^3 + L(x+y+z)^3}{(x+y)(y+z)(z+x)} = (A+R)\left(A+\rho(R)\left(A+\rho^2(R)\right)\right).$$

So it means that the polynomial ϕ associated to $L(x)^3$ divides ϕ_f, which proves the second part of proposition 1.

□

We can now complete the proof of theorem 9 by showing that f is CCZ-equivalent to a polynomial of degree e.

5. CCZ-equivalence

Let us consider $c_1 \in \mathbb{F}_{q^3}$ such that $\operatorname{tr}(c_1) = 0$ and $R(x,y,z) = c_1\phi_5 + c_1^3, \in \mathbb{F}_{q^3}[x,y,z]$. We recall that $L(x) = x(x+c_1)(x+\rho(c_1))\left(x+\rho^2(c_1)\right)$.

Theorem 11. *Let f be a function such that* $\deg(f) = 4e$, *with* $e > 3$ *such that* ϕ_e *is absolutely irreducible, and such that the polynomials of the form*

$$(x+y)(x+z)(y+z) + R,$$

divides ϕ, therefore f is CCZ-equivalent to $x^e + S(x)$, where $S \in \mathbb{F}_q[x]$ is of degree at most $e-1$.

Proof. Let us consider the set G of the polynomials of the form $g(x) = L(x)^e + S(L(x))$, where S is a polynomial of $\mathbb{F}_q[x]$ of degree at most $e-1$ with no monomials of exponent a power of 2. Let δ be the number of power of 2 less or equal than $e-1$. It is easy to remark that G defines an affine subspace of the vector space $\mathbb{F}_q[x]$ of dimension $e-\delta$. We denote by ϕ_g the polynomial ϕ associated to g and ϕ_{L^n} the polynomial ϕ associated to L^n. So we have

$$\phi_g = \phi_{L^e} + S(\phi_{L^i}).$$

Now let us consider the set F of all the polynomials f of degree $4e$ with leading coefficient 1 such that ϕ_{L^3} divides their associated polynomials ϕ and such that f does not have any monomial of exponent a power of 2. The goal of this proof is to show that $F = G$. We begin by proving that $G \subset F$, then we show that they have the same dimension.

Lemma 5. *The set G is a subset of F.*

Proof. It is sufficient to prove that ϕ_{L^3} divides ϕ_{L^n} for all $n \geqslant 3$.

We know that $x^3+y^3+z^3+(x+y+z)^3 = A$ divides $x^n+y^n+z^n+(x+y+z)^n$. Putting

$$X = L(x)$$
$$Y = L(y)$$
$$Z = L(z)$$

we have $X^3+Y^3+Z^3+(X+Y+Z)^3$ divides $X^n+Y^n+Z^n+(X+Y+Z)^n$. As $\operatorname{tr}(c_1) = 0$, $L(x)$ is a linearized polynomial so $X+Y+Z = L(x)+L(y)+L(z) = L(x+y+z)$ therefore $L(x)^3+L(y)^3+L(z)^3+L(x+y+z)^3$ divides $L(x)^n+L(y)^n+L(z)^n+L(x+y+z)^n$ then ϕ_{L^3} divides ϕ_{L^n}. □

Lemma 6. *F defines an affine subspace of the vector space $\mathbb{F}_q[x]$ of dimension less or equal than $e-\delta$.*

Proof. We consider the mapping:

$$\begin{aligned} \varphi : \quad & F \to \mathbb{F}_q^{e-\delta} \\ & f \to (a_{d-4}, \ldots, a_{12}) \end{aligned}$$

It is sufficient to prove that this mapping is one-to-one.

Let f and f' in F be two elements such that $\varphi(f) = \varphi(f')$. We write $f = \sum_{i=0}^{d} a_i x^i$ and $f' = \sum_{i=0}^{d} a'_i x^i$. We note $a_k \phi_k = \sum_{i=0}^{9} P_i Q_{k-i-3}$ and $a'_k \phi_k = \sum_{i=0}^{9} P_i Q'_{k-i-3}$.

We will show by induction that $a_i = a'_i$ for all $0 \leqslant i \leqslant d$ and that $Q_i = Q'_i$ for all $0 \leqslant i \leqslant d-12$.

We have $a_d = a'_d = 1$ and $Q_{d-12} = Q'_{d-12} = \phi_e^4$.

Suppose that $a_j = a'_j$ and that $Q_{j-12} = Q'_{j-12}$ for $j > i$. Let us show that $a_i = a'_i$ and $Q_{i-12} = Q'_{i-12}$ if 4 does not divide i.

If $i \geqslant 12$, we have

$$a_i \phi_i = \sum_{\sup(0, i-d+9)}^{9} P_k Q_{i-k-3} = A^3 Q_{i-12} + \sum_{\sup(0, i-d+9)}^{8} P_k Q_{i-k-3},$$

so A^3 divides

$$a_i \phi_i + \sum_{\sup(0, i-d+9)}^{8} P_k Q_{i-k-3}.$$

It divides

$$a'_i \phi_i + \sum_{\sup(0, i-d+9)}^{8} P_k Q'_{i-k-3} = a'_i \phi_i + \sum_{\sup(0, i-d+9)}^{8} P_k Q_{i-k-3},$$

because $i-k-3 \geqslant i-11$. So it divides $(a_i + a'_i)\phi_i$. If 4 does not divide i then A^3 does not divide ϕ_i so $a_i = a'_i$ and

$$Q_{i-12} = \frac{a_i \phi_i + \sum_{\sup(0, i-d+9)}^{8} P_k Q_{i-k-3}}{A^3} = \frac{a'_i \phi_i + \sum_{\sup(0, i-d+9)}^{8} P_k Q'_{i-k-3}}{A^3} = Q'_{d-12}.$$

□

From lemma 5 and 6 we obtain $F = G$. So every $f \in F$ is of the form $L(x)^e + S(L(x))$ and hence they are CCZ-equivalent to $x^e + S(x)$. If f is of degree $4e$ with leading coefficient 1 such that ϕ_{L^3} divides their associated polynomials ϕ and has monomials of exponent a power of 2, then f is CCZ-equivalent to a polynomial in F therefore it is also CCZ-equivalent to $x^e + S(x)$. □

We now have that f is CCZ-equivalent to a polynomial of degree e which is odd. As e is odd and not a Gold or Kasami number (see remark 2), we can deduce from theorem 1 that f cannot be an Exceptional APN function. Contradiction.

References

[1] Y. Aubry, G. McGuire, F. Rodier, A few more functions that are not APN infinitely often, Finite Fields Theory and applications, Ninth International conference Finite Fields and Applications, McGu et al.editors, Contemporary Math. n°518, AMS, Providence (RI), USA, 2010, pp23-31.

[2] T. Berger, A. Canteaut, P. Charpin, Y. Laigle-Chapuy On almost perfect nonlinear functions over $\mathbb{F}_{2^n}$. IEEE Trans. Inform. Theory 52 (2006), no. 9, 4160-4170.

[3] Biham, E. and A. Shamir. (1990). Differential Cryptanalysis of DES-like Cryptosystems. Advances in Cryptology CRYPTO '90. Springer-Verlag. 221.

[4] N. Bourbaki, Élments de mathmatique, Algbre. Springer-Verlag Berlin Heidelberg 2007

[5] L. Budaghyan and C. Carlet and P. Felke and G. Leander An infinite class of quadratic APN functions which are not equivalent to power mappings, Cryptology ePrint Archive, n° 2005/359.

[6] Byrne E. and McGuire G., Quadratic Binomial APN Functions and Absolutely Irreducible Polynomials, eprint arXiv:0810.4523 [math.NT].

[7] C. Carlet, P. Charpin and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like crypto-systems. Designs, Codes and Cryptography, 15(2), pp. 125-156, 1998.

[8] F. Caullery, Polynomial functions of degree 20 which are not APN infinitely often. eprint arXiv:1212.4638.

[9] J. Dillon, APN Polynomials: An Update. Fq9, International Conference on Finite Fields and their Applications July 2009.

[10] M. Delgado, H. Janwa, On the Conjecture on APN Functions, eprint arXiv:1207.5528

[11] Dobbertin, Hans; Mills, Donald; Muller, Eva Nuria; Pott, Alexander; Willems, Wolfgang; APN functions in odd characteristic. Combinatorics 2000 (Gaeta). Discrete Math. 267 (2003), no. 1-3, 95112.

[12] Y. Edel, G. Kyureghyan and A. Pott. A new APN function which is not equivalent to a power mapping. IEEE Trans. Inform. Theory 52 (2006), no. 2, 744-747.

[13] Y. Edel, A. Pott. A new almost perfect nonlinear function which is not quadratic Adv. Math. Commun.3 (2009), no. 1, 59-81.

[14] E. Ferard, R. Oyono and F. Rodier. Some more functions that are not APN infinitely often. The case of Gold and Kasami exponents. accepted in Proceedings of AGCT 13, March 2012.

[15] Hernando, Fernando; McGuire, Gary Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions. J. Algebra 343 (2011), 7892.

[16] H. Janwa, G. McGuire and R. M. Wilson, Double-error-correcting codes and absolutely irreducible polynomials over $GF(2)$, Journal of Algebra vol. 178, 665-676, Academic Press, 1995.

[17] H. Janwa and R. M. Wilson, Hyperplane sections of Fermat varieties in $\mathbb{P}^3$ in char. 2 and some applications to cyclic codes, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Proceedings AAECC-10 (G Cohen, T. Mora and O. Moreno Eds.), 180-194, Lecture Notes in Computer Science, Vol. 673, Springer-Verlag, New York/Berlin 1993.

[18] Browning, K. A.; Dillon, J. F.; McQuistan, M. T.; Wolfe, A. J. An APN permutation in dimension six. Finite fields: theory and applications, 3342, Contemp. Math., 518, Amer. Math. Soc., Providence, RI, 2010.

[19] G. Leander and F. Rodier Bounds on the degree of APN Polynomials. The case of $x^{-1}+g(x)$. Designs, Codes and cryptography. 0925-1022. 2009.

[20] E. Leducq, New families of APN functions in characteristic 3 or 5, Arithmetic, Geometry, Cryptography and Coding Theory, Contemporary Mathematics, AMS, 2012, 574, 115-123.

[21] Ness, Geir Jarle; Helleseth, Tor A new family of ternary almost perfect nonlinear mappings. IEEE Trans. Inform. Theory 53 (2007), no. 7, 25812586.

[22] K. Nyberg, Differentially uniform mappings for cryptography, Advances in cryptology-Eurocrypt '93 (Lofthus, 1993), 55-64, Lecture Notes in Comput. Sci., VOl. 765, Springer, Berlin, 1994.

[23] Poinsot, Laurent; Pott, Alexander Non-Boolean almost perfect nonlinear functions on non-Abelian groups. Internat. J. Found. Comput. Sci. 22 (2011), no. 6, 13511367.

[24] F. Rodier Borne sur le degr des polynmes presque parfaitement non-linaires, arXiv:math/0605232

[25] F. Rodier, Functions of degree 4e that are not APN infinitely often. Cryptogr. Commun. 3 (2011), n°4, 227-240.

[26] Zha, ZhengBang; Wang, XueLi; Power functions with low uniformity on odd characteristic nite elds. Sci. China Math. 53 (2010), no. 8, 19311940.1869-1862.
[27] Zha, Zhengbang; Wang, Xueli; Almost perfect nonlinear power functions in odd characteristic. IEEE Trans. Inform. Theory 57 (2011), no. 7, 48264832.1557-9654.